Chapter 3: Kerberos Principals and Passwords

In this chapter we discuss choosing and obtaining a strengthened realm userid (called a *Kerberos principal*) and a Kerberos password.

3.1 Your Kerberos Principal

In order to access a machine in the FNAL.GOV realm, you need to have a special identifier for the realm, called a *Kerberos principal*[1], and an associated Kerberos password. A principal is essentially a realm userid, used for authentication to the realm. You must have a valid Fermilab ID in order to get one. In addition to a principal, you must have an account on each machine that you plan to use in the realm. There are significant conveniences if your principal and your account name are the same, as we discuss in section 3.1.1 *Choosing a Principal Name*.

The system administrator of a strengthened machine may require that authorized users obtain a *<username>/root* instance of their Kerberos principal in order to access sensitive accounts on the system. The root instance has tighter restrictions placed on it (see section 9.2 *Ticket Management*). If your sytem administrator tells you it's required, use the same form as indicated in section 3.1.2 *Requesting a Principal* to request one.

3.1.1 Choosing a Principal Name

The Kerberos Strong Authentication system is expanding to include all computer systems across the site. Your Kerberos principal will be used for authentication sitewide. It is to your benefit to have one login id (account name) common to all systems that you use, and for that login id to match your Kerberos principal. The Computing Division is strongly encouraging this

[1] Note for sysadmins: if you have an account and a standard UNIX password (in the `passwd` file or NIS map) on a Kerberized machine, but no principal or Kerberos password, you can still log in and use non-Kerberized services. You can do this only at the console. (From any other terminal, the Kerberized system responds in portal mode, described in section 5.5 *Connecting from a NonKerberized Machine: Portal Mode*, and you have no option to enter your UNIX password.)

practice for ease of use. (For users new to Fermilab, your FNAL email address and your login name for all machines will be created to match your principal, by default.) With this in mind, we provide the following guidelines for choosing a Kerberos principal:

New principals should be chosen to be eight or fewer characters, and may include a variety of characters. Please use only lowercase letters (and optionally any numbers 0 through 9). **Do not use the characters "at" (`@`), forward slash (`/`), or period (`.`) in principal names**.

In Appendix C: *More about Choosing a Principal Name*, we present information for users who have pre-existing account names and/or an email address at Fermilab, and for whom the above guidelines are not straightforward to follow.

3.1.2 Requesting a Principal

Use the online *Form to Request Kerberos Principal and/or Related Items* at `http://www.fnal.gov/cd/forms/strongauth.html`. Guidance is provided on the form as to which items you may need in addition to a principal.[1]

3.2 Your Kerberos Password

Once your request for a principal on the FNAL.GOV realm has been approved, you must stop by WH8NE (Yolanda Valadez' office) to receive your initial Kerberos password. An exception is granted for off-site visitors (whose Fermilab ID is a VID): you can get it over the telephone (630-840-8118); you will be asked a question to verify your identity.[2]

☞ You are required to change the initial password within 30 days of receipt, and once a year (actually every 400 days) thereafter.

[1] Note that if you obtained a principal for the PILOT.FNAL.GOV realm, you do **not** need to get a new principal (or password) for the transition from the PILOT.FNAL.GOV realm to FNAL.GOV.

[2] For principals that were migrated from the PILOT.FNAL.GOV realm to the production realm on May 10, 2001, the existing pilot realm password and expiration date were replicated in the production realm. A password *change* in one realm after that date will not be reflected in the other realm.

Even if you use a CRYPTOCard exclusively, you need to change your Kerberos password as stated above in order to continue accessing machines in the FNAL.GOV realm!

3.2.1 Important! Please Read!

Please treat your Kerberos password as an inviolable object. Never give your password to anybody for any reason. Doing so constitues a policy violation. If you really need to give someone access to your account (this practice is discouraged, by the way), add the person's principal to your `.k5login` or `.k5users` file as described in section 9.3 *Account Access by Multiple Users*.

Typing in your Kerberos password should ideally be done infrequently (i.e., no more than once each day). Do not type it in carelessly. You are allowed to type your Kerberos password over an **encrypted** link on an occasional basis (e.g., when initially changing your password), however as a regular practice, please authenticate locally and forward your credentials to remote systems.

Windows 2000 domain-only users: type your password **only** at the Windows login prompt.

3.2.2 Choosing a Kerberos Password

In contrast to the principal (which ideally should match your login name on each machine and your email address), your Kerberos password must be unique. That is, in order to avoid exposing your Kerberos password, it must be different from the passwords you use for any other purpose (with the single exception of your Fermilab Windows 2000 domain Kerberos password).

The Fermilab Computer Security Team has imposed some restrictions on passwords in accordance with DOE guidelines. Currently, a password for the FNAL.GOV strengthened realm is required to contain a minimum of ten characters from at least two of the following five classes: lowercase letters, uppercase letters, numbers, punctuation, and all other characters. Passwords for /root principals must contain a minimum of 11 characters including at least three of the five classes. Passwords the system considers "bad" will be rejected. (Passwords are checked against the "cracklib" dictionary, which will often surprise you by its thoroughness!)

Need some ideas for thinking up a good password?[1] Remember, a good password is one you can remember, but that no one else can easily guess. Examples of passwords that would be good *if they weren't listed in this manual* include:

[1] These ideas were lifted from MIT's Kerberos V5 User's Guide (C) 1996, local copy stored at `http://www-dcd.fnal.gov/computersecurity/StrongAuth/UserDocs/user-guide.html`.

- some initials, like “GykoR-66.” for “Get your kicks on Route 66.”
- an easy-to-pronounce nonsense word, like “slaRooBey” or “krang-its”
- a misspelled phrase, like “2HotPeetzas!” or “ItzAGurl!!!”

Note: Don’t actually use any of the above passwords. They’re only meant to show you how to make up a good password. Passwords that appear in a manual are the first ones intruders will try.

3.2.3 Changing your Kerberos Password

If possible, change your password at the console of a machine, not over a network connection. If this is not possible, then before changing your password, **verify that you are using an encrypted connection!** How do you know if your connection is encrypted? See Chapter 11: *Encrypted vs. Unencrypted Connections* for some help.

☞ We repeat: You are required to change your initial password within 30 days of its creation and roughly once a year thereafter in order to continue having access to machines in the strengthened realm, no matter what access method you use. The **kinit** program warns you if your password is within 30 days of its expiration date, and as of **kerberos** v1_2, the **kerberos** login program includes this warning as well.

The Computing Division has set up terminals in two locations for people to change their Kerberos passwords. There is one terminal outside of WH8NE, another is in the email center in Wilson Hall, ground floor, north end.

If you don’t have a secure connection over which to change your password, find someone who does, and borrow his or her command prompt (yes, you can change it from someone else’s account; just give your principal name as an argument).

If your initial password expires, you can still change it as long as you remember what it was, but you cannot use CRYPTOCard access while it remains expired. If you forget your initial password before you get around to changing it, stop by WH8NE (or off-site call 630-840-8118) and ask Yolanda Valadez to reset it (but please try to change it right away!).

UNIX/Linux/Cygwin

To change your password, run the **`kpasswd`** command.

AFS

On strengthened UNIX systems running AFS, there are two **`kpasswd`** commands, one for AFS and one for Kerberos. Your $PATH should be set such that the Kerberos **`kpasswd`** comes first. Kerberos is implemented at Fermilab such that your AFS tokens will be obtained automatically. If you are unsure which **`kpasswd`** is being invoked, force the system to use the Kerberos version by running **`setup kerberos`** first.

```
% setup kerberos
```

Then run **`kpasswd`**. If borrowing someone else’s account or if your principal does not match your login id, include your principal name as an argument.

```
% kpasswd [<principal_name>]
```

```
kpasswd: Changing password for aheavey@FNAL.GOV.
Old password:                  <--- type your initial password here.
kpasswd: aheavey@FNAL.GOV’s password is controlled by the policy default,
which
requires a minimum of 10 characters from at least 2 classes (the five classes
are lowercase, uppercase, numbers, punctuation, and all other characters).
New password:                  <--- type your new password here.
New password (again):          <--- type your new password here for confirmation.
Kerberos password changed.
```

If you choose a password that is too short, you will see this error message:

```
kpasswd: New password is too short.
Please choose a password which is at least 10 characters long.
```

If it’s long enough but you haven’t met the multiple-class requirement, you’ll see:

```
kpasswd: New password does not have enough character classes.
The character classes are:
        - lower-case letters,
        - upper-case letters,
        - digits,
        - punctuation, and
        - all other characters (e.g., control characters).
Please choose a password with at least 2 character classes.
```

If the password has expired, you’ll need to get access to a machine running **`kpasswd`** some other way (e.g., find a friend or use a local account) to change it.

Windows (with WRQ® Reflection software installed)

Here we assume you are running the **WRQ® Reflection** software for **Windows** as described in Chapter 19: *Installing and Configuring WRQ® Reflection on a Windows System*. To change your Kerberos password via the **Reflection** application:

- (If you run W2K or NT4, and installed WRQ® using the automated script, skip this first step.) First update the Windows services file by executing `\\Pckits\WRQ\services.bat`. For Win95 or 98, you must copy it manually from `\\Pckits\WRQ\` (target directory may vary).
- Next, navigate to **START** > **PROGRAMS** > **REFLECTION** > **UTILITIES** > **KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application. From the **TOOLS** menu select **CHANGE PASSWORD...** and change it.

Windows (with Exceed 7.0 and MIT Kerberos)

Here we assume you are running **Exceed 7** with the **MIT Kerberos** software for Windows as described in Chapter 22: *Installing and Configuring MIT Kerberos on Windows, for use with Exceed 7*.

Note: The **CHANGE PASSWORD** utility in **Leash32** does not work, and **`kpasswd`** in the Command Prompt works for the AFS password. Consequently, changing your password under this configuration requires typing your password over a network connection. Try to find a machine on which you can do it locally, instead. Only use this as a last resort.

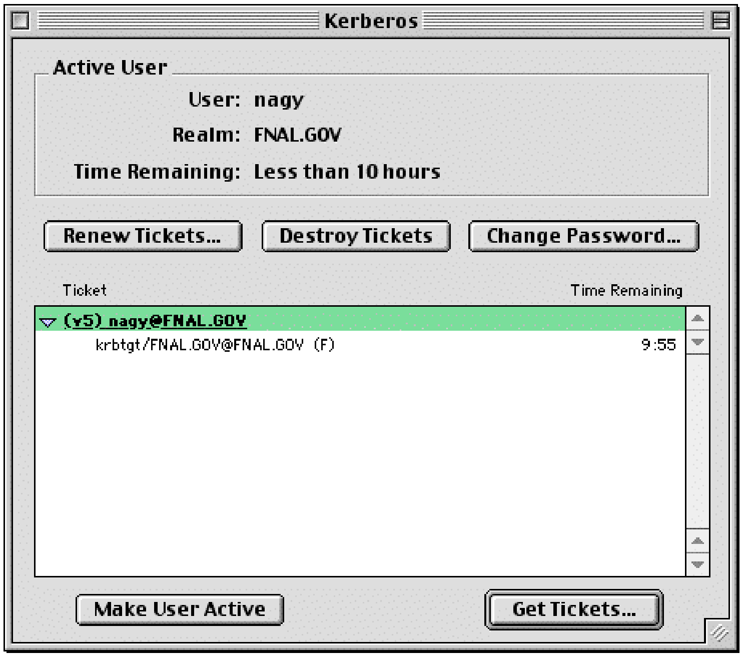
To change your Kerberos password:

Make your connection to your UNIX host using a telnet profile with Kerberos enabled as outlined in section 22.5 *Configuring the Exceed 7 Telnet Application*. Verify that encryption is set. Use the **`kpasswd`** command to change your Kerberos password, as described for UNIX, earlier in this section.

Macintosh

Here we assume you are running the **MIT Kerberos** software for Macintosh as described in Chapter 24: *Installing and Configuring MIT Kerberos on a Macintosh System*. To change your Kerberos password:

1) Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the **KERBEROS CONTROL STRIP** module).



Active User

User: nagy

Realm: FNAL.GOV

Time Remaining: Less than 10 hours

Ticket	Time Remaining
(v5) nagy@FNAL.GOV	
krbtgt/FNAL.GOV@FNAL.GOV (F)	9:55

2) Select a username and realm and click **GET TICKETS** for which you will have to provide your current (or initial) Kerberos password.

3) Click on the ticket to highlight it, then click **CHANGE PASSWORD** and enter the old and new passwords on the pop-up screen which appears.